L'attaque de l'homme du milieu en cybersecurité

Pr Chérif DIALLO, CISSP
Professeur Titulaire des Universités
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" Si le premier commandement de l'enquêteur est d'écouter, celui de l'espion est de se faire oublier." Jean Michel Riou.

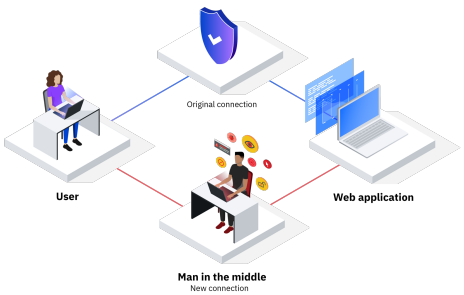
Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui la problématique des attaques de l'homme du milieu. Après une brève définition, ce bulletin présente le cycle d'une attaque de l'homme du milieu avant de lister quelques stratégies de protection à adopter pour faire face à ces menaces.

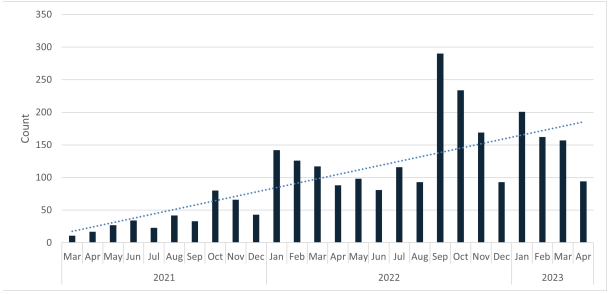
Mots clés : Attaque de l'homme du milieu, Ingénierie sociale, hameçonnage (phishing), spam.

---

1. Définition

On la connaît sous de nombreux noms : monster in the middle attack, man in the middle attack, MitM, attaque de l'intercepteur ou encore attaque de l'homme du milieu. Elle est, ainsi, une forme de cyberattaque dans laquelle les criminels exploitant des failles de protocoles s'insèrent entre les entités d'un canal de communication pour voler des données.





Nombre de campagnes de phishing de type « man-in-the-middle » par mois

Une attaque de l'homme du milieu (MitM) est un terme générique désignant une attaque où l'attaquant se place au milieu d'une conversation, soit pour espionner, soit pour se faire passer pour l'une des parties, donnant l'impression qu'un échange d'informations normal est en cours.

L'objectif d'une attaque MitM est de voler des informations personnelles, telles que les identifiants de connexion, les détails de compte et les numéros de carte de crédit. Les cibles sont généralement les utilisateurs d'applications financières, les entreprises SaaS, les sites de commerce électronique et autres sites web nécessitant une connexion. Les informations obtenues peuvent alors être utilisées à de nombreuses fins, notamment l'usurpation d'identité, les transferts de fonds non autorisés ou la modification illicite d'un mot de passe. Elles peuvent également servir à s'introduire dans un périmètre sécurisé lors de la phase d'infiltration d'une attaque de menace persistante avancée (APT). Voici quelques cas illustratifs d'attaques de l'homme du milieu :

- ***Tesla*** : En 2024, des chercheurs en sécurité ont signalé qu'une vulnérabilité permettait aux pirates de lancer une attaque MITM pour déverrouiller et voler des véhicules Tesla. En utilisant un point d'accès Wi-Fi usurpé dans une station de recharge Tesla, un pirate informatique pourrait collecter les identifiants de compte d'un propriétaire de Tesla. Selon les chercheurs, l'attaquant pourrait alors ajouter une nouvelle « clé téléphonique », qui déverrouille et démarre le véhicule à l'insu de son propriétaire.
- ***Reddit*** : Un récent incident survenu en 2023 a ciblé le réseau social américain Reddit, sous la forme d'une attaque de phishing sophistiquée dirigée spécifiquement contre l'un des employés de la société. Celui-ci ayant cliqué sur un lien qui lui avait été envoyé s'est trouvé redirigé vers un portail Intranet imitant à la perfection celui de Reddit. Il a saisi ses informations de connexion sans se douter que des hackers étaient

en train de les récupérer. Cette attaque s'est soldée par la compromission des coordonnées de centaines de collaborateurs.

- ***Microsoft Office 365*** : En 2022, des chercheurs en sécurité ont découvert une vaste campagne de compromission des e-mails professionnels. Cette attaque de l'homme du milieu a piégé plus de 10 000 entreprises en usurpant la page de connexion de Microsoft 365. Les attaquants se servaient d'une solution qui faisait tampon entre le formulaire de connexion légitime à Microsoft 365 et une page de phishing, afin de voler les informations d'identification et le cookie de session généré lors de la demande d'authentification multifacteur. Suite à cette découverte, Microsoft s'est appuyée sur cet incident pour rédiger un rapport (en anglais) avec des explications sur le mode d'action utilisé et des recommandations pour aider les entreprises à se protéger de ce type d'attaques.
- ***OTAN*** : En septembre 2022, le piratage de l'État-major des Forces armées portugaises a eu des retombées à grande échelle. La violation de données a, en effet, provoqué la fuite de documents de l'OTAN classifiés comme secrets et confidentiels, ainsi que leur mise en vente sur le Dark Web. Cette affaire extrêmement grave a suscité beaucoup d'inquiétudes sur la scène internationale. L'enquête a révélé que la violation de données était due à une sécurisation insuffisante des moyens de communication utilisés, une faille critique qui a permis aux attaquants de dérober ces informations. Cette cyberattaque est d'autant plus troublante qu'elle était totalement indétectable : pendant longtemps, les attaquants ont travaillé dans l'ombre, collectant toutes les données partagées via des canaux non sécurisés.
- ***Les attaques MitM*** ont contribué à des violations de données massives. Les plus grandes violations de données en 2021 comprenaient Cognyte (cinq milliards d'enregistrements), Twitch (cinq milliards d'enregistrements), LinkedIn (700 millions d'enregistrements) et Facebook (553 millions d'enregistrements).
- ***Equifax*** : En 2017, l'agence d'évaluation du crédit Equifax a été victime d'une attaque de type homme au milieu en raison d'une vulnérabilité non corrigée dans son framework d'applications web. L'attaque a révélé les informations financières de près de 150 millions de personnes. Dans le même temps, Equifax a découvert des failles de sécurité dans ses applications mobiles susceptibles d'exposer ses clients à de nouvelles attaques MitM. Equifax a supprimé ces applications de l'App Store d'Apple et de Google Play.
- ***DigiNotar*** : En s'appuyant sur de faux sites Web pour collecter des mots de passe, des pirates ont lancé avec succès une attaque MitM contre l'autorité néerlandaise de sécurité numérique DigiNotar en 2011. La faille était importante, car DigiNotar a émis plus de 500 certificats de sécurité compromis à de grands sites web tels que Google, Yahoo! et Microsoft. DigiNotar a finalement perdu sa licence en tant que fournisseur de certificats de sécurité et a été déclaré en faillite.

2. Cycle d'une attaque de l'homme du milieu

Quelles que soient les techniques spécifiques ou la pile de technologies nécessaires pour mener une attaque MitM, il existe un ordre de travail de base :

- La personne A envoie un message à la personne B.
- L'attaquant MitM intercepte le message à l'insu de la personne A ou de la personne B.
- L'attaquant MitM modifie le contenu du message ou le supprime complètement, encore une fois, à l'insu de la Personne A ou de la Personne B.

Donc, on voit bien qu'il s'agit d'abord d'une interception, suivie ensuite d'une phase de déchiffrement et modification. Ces deux étapes constituent en général le cycle d'une attaque MitM :

- ***Interception*** : Afin de se placer au milieu de deux cibles communicantes, comme un utilisateur et une application Web, un pirate doit intercepter les données qui circulent entre les deux. L'attaquant transmet ensuite ces informations détournées entre les cibles comme si des communications normales étaient en cours, de sorte que les victimes ne se doutent de rien. Les attaquants souhaitant adopter une approche plus active en matière d'interception peuvent lancer l'une des attaques suivantes :
  - ***IP Spoofing*** : L'usurpation d'adresse IP consiste pour un attaquant à se faire passer pour une application en modifiant une adresse IP (le plus souvent l'adresse du destinataire) dans les en-têtes de paquets. Ainsi, les utilisateurs qui tentent d'accéder à une URL connectée à l'application sont redirigés vers le site web de l'attaquant.
  - ***ARP Spoofing*** : L'usurpation ARP consiste à lier l'adresse MAC d'un attaquant à l'adresse IP d'un utilisateur légitime sur un réseau local à l'aide de faux messages ARP. Ainsi, les données envoyées par l'utilisateur à l'adresse IP de l'hôte sont transmises à l'attaquant.
  - ***DNS Spoofing*** : L'usurpation DNS, également appelée empoisonnement du cache DNS, consiste à infiltrer un serveur DNS et à modifier l'enregistrement d'adresse d'un site web. Ainsi, les utilisateurs qui tentent d'accéder au site sont redirigés vers le site de l'attaquant par l'enregistrement DNS modifié.
- ***Déchiffrement*** : La plupart des communications internet sont aujourd'hui chiffrées, de sorte que toutes les données interceptées par un attaquant MITM devront très probablement être décryptées avant que le pirate ne puisse les utiliser. Les attaquants peuvent déchiffrer les données en volant des clés de

chiffrement, en exécutant des attaques par force brute ou en utilisant des techniques d'attaque MITM spécialisées. Ainsi, après interception, tout trafic SSL bidirectionnel doit être déchiffré sans alerter l'utilisateur ou l'application. Plusieurs méthodes permettent d'y parvenir :

- ***HTTPS Spoofing*** : L'usurpation HTTPS envoie un faux certificat au navigateur de la victime dès la première demande de connexion à un site sécurisé. Ce certificat contient une empreinte numérique associée à l'application compromise, que le navigateur vérifie à partir d'une liste de sites de confiance. L'attaquant peut alors accéder aux données saisies par la victime avant leur transmission à l'application.
- ***SSL BEAST*** (exploit de navigateur contre SSL/TLS) cible une vulnérabilité TLS version 1.0 de SSL. L'ordinateur de la victime est alors infecté par un code JavaScript malveillant qui intercepte les cookies chiffrés envoyés par une application web. Le chaînage de blocs de chiffrement (CBC) de l'application est ensuite compromis afin de déchiffrer ses cookies et ses jetons d'authentification.
- ***SSL Hijacking*** : Le piratage SSL se produit lorsqu'un attaquant transmet de fausses clés d'authentification à l'utilisateur et à l'application lors d'une négociation TCP. Cela établit une connexion apparemment sécurisée alors qu'en réalité, l'homme du milieu contrôle l'intégralité de la session.
- ***SSL Stripping*** : Le décryptage SSL rétrograde une connexion HTTPS en HTTP en interceptant l'authentification TLS envoyée par l'application à l'utilisateur. L'attaquant envoie alors une version non chiffrée du site de l'application à l'utilisateur tout en maintenant la session sécurisée avec l'application. Parallèlement, l'intégralité de la session de l'utilisateur est visible par l'attaquant.

3. Solutions : comment éviter une attaque de l'homme du milieu ?

Étant donné que les attaques MitM reposent sur des éléments plus étroitement associés à d'autres cyberattaques, tels que le phishing ou l'usurpation d'identité, des activités malveillantes que les employés et les utilisateurs peuvent avoir déjà été formés à reconnaître et à contrecarrer, les attaques MitM peuvent, à première vue, sembler faciles à repérer. Le fait de savoir reconnaitre les signes d'une attaque MitM est important. Voici quelques signes indiquant qu'il peut y avoir des écoutes clandestines sur votre réseau et qu'une attaque MitM est en cours :

- ***Déconnexions inhabituelles***. Les déconnexions inattendues ou répétées d'un service, lorsqu'un utilisateur est étrangement mis hors service et doit se connecter encore et encore, sont généralement le signe d'une tentative ou d'une attaque MitM.
- ***URL étranges***. Dans une escroquerie à l'usurpation d'identité, les cybercriminels créent des faux sites Web qui semblent identiques à ceux qui sont reconnaissables et de confiance pour inciter les victimes à saisir leurs identifiants. Dans la version MitM de cette attaque, la page Web fournie à l'utilisateur dans son navigateur est un site usurpé, et l'URL dans la fenêtre d'adresse n'est clairement pas l'adresse reconnaissable du site ou de l'application de confiance. Les attaquants MitM utilisent un détournement DNS afin que les utilisateurs interagissent et s'engagent avec le site usurpé tandis que le code malveillant intercepte leurs messages et collecte leurs données. Pour toutes les transactions financières personnelles, les utilisateurs doivent examiner attentivement les pages Web de leurs institutions financières pour déterminer si quelque chose semble inconnu.
- ***Wi-Fi public et non sécurisé***. Le Wi-Fi public disponible auprès d'établissements inconnus doit être évité si possible. Cela est différent du Wi-Fi municipal, qui est une connectivité gratuite offerte par les villes afin que les résidents puissent se connecter à Internet. Même si les utilisateurs n'effectuent pas de transactions bancaires ou d'autres tâches impliquant des données sensibles sur un Wi-Fi public, une attaque MitM peut toujours envoyer du code malveillant à un appareil pour écouter des chats et des messages. Les criminels sont connus pour utiliser des noms de réseau Wi-Fi innocents, tels que « Local Free Wireless », alors faites attention. Les attaquants offrent peut-être une connectivité gratuite, mais ils observent également toute l'activité de l'utilisateur.

Il existe des mesures de cybersécurité que les organisations et les particuliers peuvent mettre en œuvre pour se protéger contre les attaques de type homme au milieu. Les experts recommandent de se concentrer sur des stratégies parmi lesquelles on pourrait citer les suivantes :

- ***Ne cliquez jamais sur les liens repris dans les e-mails ou les SMS.*** Prenez l'habitude de toujours saisir manuellement l'adresse Internet dans la barre d'adresse, et ce quel que soit l'expéditeur du message. Faites toutefois l'effort de rechercher une version officielle de l'adresse Internet en question. Ne cliquez jamais sur une adresse Internet avant d'avoir confirmé s'il s'agissait d'une adresse officielle ou légitime.
- ***Utilisez l'authentification à plusieurs facteurs.*** Chaque fois que vous le pouvez, ayez recours à une authentification multifacteur (MFA). Celle-ci renforce la sécurité puisque le mot de passe ne suffit pas pour obtenir l'accès aux données. Confrontés à la MFA, les attaquants auront beaucoup plus de mal à se faire passer pour vous.

- ***Connectez-vous à des réseaux sécurisés.*** Ne vous connectez pas à n'importe quel réseau. Lorsque vous souhaitez consulter des informations sensibles ou effectuer des transactions financières, faites-le depuis un réseau sécurisé et fiable. Évitez les réseaux WiFi publics : ils sont souvent la cible d'attaques MitM.
- ***Utilisez un réseau privé virtuel (VPN).*** Utilisez un VPN fiable, en particulier si vous vous connectez à des réseaux Wi-Fi publics. Ces outils VPN cryptent votre trafic et les liaisons via des serveurs sécurisés ce qui complique considérablement la tâche de pirates informatiques qui chercheraient à intercepter ou à manipuler vos données.
- ***Formation, communication et sensibilisation.*** Dans le cadre d'une entreprise, il est essentiel de sensibiliser les employés aux questions de cybersécurité. Encouragez-les à signaler rapidement toute anomalie survenant sur le réseau, tout message d'erreur ou problème de sécurité qu'ils peuvent rencontrer : c'est ce qui vous permettra de mettre en place une ligne de défense collective contre les menaces d'attaques MitM.
- ***HTTPS***. Les utilisateurs ne doivent visiter que des sites web disposant d'une connexion sécurisée, qui sont indiqués par « HTTPS » et une icône cadenas dans la barre d'adresses du navigateur. Les pages web qui n'offrent que des connexions HTTP non sécurisées doivent être évitées. En outre, les protocoles SSL et Transport Layer Security (TLS) pour les applications peuvent protéger contre le trafic web malveillant et empêcher les attaques par usurpation d'identité.
- ***Adopter la philosophie Zero Trust***. Le Zero Trust est un concept de sécurité qui exige des organisations qu'elles ne fassent pas automatiquement confiance à quoi que ce soit à l'intérieur ou à l'extérieur de leurs périmètres. Au contraire, ils doivent d'abord vérifier tout ce qui tente de se connecter à leurs systèmes avant d'accorder l'accès. Le modèle n'est « jamais fiable, toujours vérifier » et repose sur une vérification continue sur tous les appareils, utilisateurs et applications. Les approches Zero Trust peuvent empêcher une attaque MitM de démarrer ou peuvent protéger les actifs d'une organisation si une attaque MitM est déjà en cours.

4. En conclusion

" Le numérique crée une situation où il n'y a plus de secrets." Angela Merkel.

L'attaque de l'homme du milieu, est un type de cyberattaque où le pirate détourne les informations d'un utilisateur à son insu. Les attaques MitM sont souvent dues à des implémentations vulnérables, ou l'utilisation de chiffrements obsolètes et non-sécurisés. Pour contrer ces risques, il est important d'utiliser un chiffrement SSL/TLS de bout en bout optimisé. Les certificats doivent être mis en œuvre de manière optimale pour prévenir les attaques compromettantes. Cela permet de sécuriser davantage le site Web et l'application Web contre les attaques de rétrogradation de protocole et les tentatives de détournement de cookies.

Au-delà des mesures de sécurité mises en œuvre, il est important de renforcer la formation et la sensibilisation des utilisateurs, car les attaques MitM sont graves et nécessitent une prévention rigoureuse. Les entreprises sont confrontées à des risques accrus en raison de la mobilité d'entreprise, des télétravailleurs, de la vulnérabilité des appareils IoT, de l'utilisation accrue des dispositifs mobile et du danger d'utiliser des connexions Wi-Fi non sécurisées.

Enfin, il faut noter que le Cybersecurity Almanac 2022, publié par le Cybercrime Magazine, a signalé 6 000 milliards de dollars de dommages causés par la cybercriminalité en 2021. Ce chiffre devrait dépasser 10 billions de dollars par an à partir de 2025.